



SAP SuccessFactors

PUBLIC

Document Version: 1H 2024 – 2024-04-19

Managing Instance Access

Content

1	Instance Access Management.	3
2	Provisioning Access Management.	4
2.1	Provisioning.	4
	Provisioning Access.	5
	Provisioning Users.	6
2.2	Viewing Users with Provisioning Access.	7
2.3	Approving a New Provisioning User.	8
2.4	Removing a Provisioning User.	10
3	Super Admin Management.	12
3.1	Super Administrators.	12
3.2	Viewing Super Admins with Access to Your System.	13
3.3	Removing a Super Admin User.	14
	Setting User Status to Inactive.	15
3.4	Creating a Super Admin User in Provisioning.	16
4	IP Restriction Management.	18
4.1	IP Restrictions.	18
4.2	Adding an IP Restriction.	19
4.3	Excluding External Users from IP Restrictions.	20
5	Support Access Management.	21
5.1	Support Access with Secondary Login.	21
5.2	Enabling Secondary Login and Support Access Management.	22
	Permission to Manage Support Access.	23
5.3	Granting Support Access to a Specified User Account.	23
5.4	Removing Support Access to User Accounts.	24
5.5	Checking Role-Based Permissions Administrator Access of a Support Account.	25
5.6	Logging In to a Support Access-Enabled Account with Secondary Login.	27
6	Session Timeout.	29

1 Instance Access Management

As an administrator, you can view and control who has access to your instance, using admin tools.

- **Manage Provisioning Access:** To view and control who is allowed to access Provisioning for your instances, and to view super admins in your system and the Provisioning user who created them.
- **IP Restriction Management:** To specify the IP addresses from which users are allowed to access your instance.
- **Manage Support Access:** To grant or remove support access to a specified user account.

2 Provisioning Access Management

As an administrator, you can view and control who has Provisioning access to your instance, using the [Manage Provisioning Access](#) tool in Admin Center.

You can view and control who is allowed to access Provisioning for your instances. As an administrator, you can view a list of users with Provisioning access to your instance and you can remove this access from anyone on the list. You can also approve the users who are allowed to request Provisioning access to your instance. Users you approve are notified by email and must submit your written approval when requesting Provisioning access to your instance.

It's a universal feature, available to all SAP SuccessFactors customers. However, it requires role-based permissions and to access this tool, you must first be granted the [View Provisioning Access](#) and the [Control Provisioning Access](#) permissions.

→ Remember

Provisioning access is instance-specific. If you've more than one instance in your SAP SuccessFactors system (Development, Test, Production), you need to manage Provisioning access separately in each instance.

[Provisioning \[page 4\]](#)

Provisioning is the process of enabling your SAP SuccessFactors solutions and setting up key features in your instance, using the SAP SuccessFactors Provisioning application.

[Viewing Users with Provisioning Access \[page 7\]](#)

View information about users who have Provisioning access to your instance. Use filters to find specific users or users with the same status.

[Approving a New Provisioning User \[page 8\]](#)

Approve a new Provisioning user to your instance and notify that user by e-mail of your approval.

[Removing a Provisioning User \[page 10\]](#)

Remove Provisioning access to your instance from one or more Provisioning users.

2.1 Provisioning

Provisioning is the process of enabling your SAP SuccessFactors solutions and setting up key features in your instance, using the SAP SuccessFactors Provisioning application.

The term "Provisioning" is also commonly used to refer to the Provisioning application itself, such as when you are told that a certain new feature "must be enabled in Provisioning." The Provisioning application is only available to approved SAP employees and partners.

Access to Provisioning is restricted for number of reasons:

- Provisioning settings may enable solutions that require the purchase of a license.
- New features are often introduced in Provisioning during the development or beta phase before they are made generally available.

- Some Provisioning settings are technical in nature or can have a significant impact if used improperly, so are restricted for use by trained SAP employees and partners only.

→ Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Product Support.

[Provisioning Access \[page 5\]](#)

Provisioning access is the ability to make changes to a specific customer instance in the Provisioning application.

[Provisioning Users \[page 6\]](#)

The Provisioning application is only available to SAP employees and partners who have specifically requested a Provisioning account. Before receiving a Provisioning account, users must complete training or demonstrate sufficient technical knowledge to ensure proper use of the Provisioning application. In order to gain Provisioning access to your specific instance, Provisioning users must submit written confirmation of your approval.

Parent topic: [Provisioning Access Management \[page 4\]](#)

Related Information

[Viewing Users with Provisioning Access \[page 7\]](#)

[Approving a New Provisioning User \[page 8\]](#)

[Removing a Provisioning User \[page 10\]](#)

2.1.1 Provisioning Access

Provisioning access is the ability to make changes to a specific customer instance in the Provisioning application.

Only approved SAP employees and partners are allowed to have Provisioning access to your instance. 2FA is now required for SAP employees and partners to access the Provisioning of customer instances. To know more about how to enable multifactor authentication, log in and see <https://support.sap.com/en/my-support/mfa.html>.

Provisioning users can request either of two types of access: long-term and short-term.

Long-term access gives a user indefinite Provisioning access to your instance. It's typically used by implementation consultants or partners involved in other long-term projects. They obtain your approval through e-mail— either directly or with a system-generated e-mail sent by the *Manage Provisioning Access* tool. For more information about long-term Customer Instance Access Requests (CAR), see [Customer Instance Access Requests](#).

Short-term access gives a user Provisioning access to your instance for 48 hours. It's typically used by Product Support to resolve specific cases. They can obtain your approval through any communication channel, while working with you on the case, and gain short-term Provisioning access through an internal request process.

⚠ Caution

Provisioning users with both short-term and long-term access appear in the [Manage Provisioning Access](#) tool.

The admin user working on a specific case might not be the same person as the admin user who manages Provisioning access using the [Manage Provisioning Access](#) tool. Provisioning users with short-term access can appear temporarily on the page while working on a case. Therefore, if you see a name that you don't recognize on the page, we recommend that you wait 48 hours and/or consult with other administrators before deleting the user.

Removing short-term Provisioning access may impede the timely resolution of your incident.

Parent topic: [Provisioning \[page 4\]](#)

Related Information

[Provisioning Users \[page 6\]](#)

[Provisioning Access Management \[page 4\]](#)

2.1.2 Provisioning Users

The Provisioning application is only available to SAP employees and partners who have specifically requested a Provisioning account. Before receiving a Provisioning account, users must complete training or demonstrate sufficient technical knowledge to ensure proper use of the Provisioning application. In order to gain Provisioning access to your specific instance, Provisioning users must submit written confirmation of your approval.

📌 Note

We recommend that you manage Provisioning access using the [Manage Provisioning Access](#) admin tool whenever possible. However, if this is not possible during the early stages of implementation, you can also provide your written approval of new Provisioning users for your instance through other means, such as email.

Some of the SAP employees who may have Provisioning access to your instance include:

- **Professional Services.** Provisioning access is required during the initial implementation of an SAP SuccessFactors system.
- **Product Support.** Provisioning access is required to make changes to the configuration of your instance, enable some new features, and investigate some issues you have reported.
- **Product Engineering and Operations.** Provisioning access may be required to investigate an issue you have reported or to roll out global changes to all customers.

Other people who may have Provisioning access to your instance include:

- SAP implementation partners
- SAP consultants and development partners

Parent topic: [Provisioning \[page 4\]](#)

Related Information

[Provisioning Access \[page 5\]](#)

2.2 Viewing Users with Provisioning Access

View information about users who have Provisioning access to your instance. Use filters to find specific users or users with the same status.

Prerequisites

You have [View Provisioning Access](#) permission.

Procedure

1. Go to ► [Admin Center](#) ► [Manage Provisioning Access](#) ►.
2. Review a list of all the users who have Provisioning access to your instance.

This list includes Provisioning users with both short-term and long-term access. Users gain temporary short-term access for 48 hours only while working on a specific case. When their access expires, they disappear from this list.

You can see the following information about each user:

- ID
 - Username
 - Email
 - Status
 - Number of super admins they've created in Provisioning
3. To find a specific user, do the following:
 - a. Click the filter icon.
 - b. In the [Include](#) section, select the filter criteria [ID](#) or [Status](#).

Note

You can only filter using the [Include](#) operation and the [equal to](#) expression. Do not use [Exclude](#) or change the expression type in the second dropdown menu.

- c. In the text field, enter the ID or status of the users you want to find.
 - To filter by ID, enter the ID of a specific user.
 - To filter by status, enter *active* or *locked*.
- d. Click *OK*.
4. To view a list of users, by status, do the following:
 - a. Click the filter icon.
 - b. In the *Include* section, select *Status* in the first dropdown menu.

ⓘ Note

Currently, you can only filter using the *Include* operation and the *equal to* expression. Do not use *Exclude* or change the expression type in the second dropdown menu.

- c. In the text field, select *Active* or *Locked* to view a list of users with that status.
 - a. Click *OK*.
5. To view more users, if the list is very long, scroll to the bottom of the page and click *More*.

Task overview: [Provisioning Access Management \[page 4\]](#)

Related Information

[Provisioning \[page 4\]](#)

[Approving a New Provisioning User \[page 8\]](#)

[Removing a Provisioning User \[page 10\]](#)

2.3 Approving a New Provisioning User

Approve a new Provisioning user to your instance and notify that user by e-mail of your approval.

Prerequisites

You have the role-based permissions [View Provisioning Access](#) and [Control Provisioning Access](#).

ⓘ Note

- The approver must be a real user with valid username and business e-mail address. System users with usernames like "sfadmin" are not supposed to provide approvals.
- The approver must have real first name and last name set in the system. The approver's full name and email address is displayed in the e-mail notification that the approved Provisioning user receives.
- To create a new user, see [Choosing a Tool for User Management](#).

Context

Access to Provisioning is strictly controlled. Only SAP employees and partners who have completed the required training are given a Provisioning user account. SAP employees and partners with a Provisioning account must also submit your written approval when requesting Provisioning access to your instance.

When you approve users in the [Manage Provisioning Access](#) tool, they do **not** immediately gain access to Provisioning for your instance. Instead, they receive an e-mail notification of your approval, which they can submit along with their Provisioning access request.

We recommend that you manage Provisioning access using the [Manage Provisioning Access](#) tool whenever possible. However, if this is not possible during the early stages of implementation, you can also provide your written approval of new Provisioning users for your instance through other means, such as e-mail.

Procedure

1. Go to [Admin Center](#) > [Manage Provisioning Access](#).
2. Click the plus icon to open the [Add New Provisioning User](#) dialog.
3. Provide the e-mail address of the user you want to add.
4. Click [Add](#).

Results

The specified Provisioning user receives an e-mail notification of your approval, which they can submit along with their Provisioning access request. Both training certification and customer approval are verified during the processing of their request. After our internal review process is completed, the approved new user gains Provisioning access to your instance.

Task overview: [Provisioning Access Management \[page 4\]](#)

Related Information

[Provisioning \[page 4\]](#)

[Viewing Users with Provisioning Access \[page 7\]](#)

[Removing a Provisioning User \[page 10\]](#)

2.4 Removing a Provisioning User

Remove Provisioning access to your instance from one or more Provisioning users.

Prerequisites

You have the role-based permissions [View Provisioning Access](#) and [Control Provisioning Access](#).

Context

⚠ Caution

The [Manage Provisioning Access](#) tool shows Provisioning users with both short-term and long-term access. As the admin user who manages Provisioning access, you may not be familiar with some Provisioning users who have been granted short-term access to work on a specific case. Provisioning users with short-term access appear temporarily while working on a case. Therefore, if you see a name you do not recognize, we recommend that you wait 48 hours or consult with other administrators before deleting the user. Removing short-term Provisioning access may impede the timely resolution of the case.

⚠ Caution

Removing Provisioning access also removes your visibility into super admin accounts created by that user. We recommend that you do **not** remove Provisioning users who have created a super admin account that is still active. If the super admin account is no longer needed, we recommend that you deactivate the user before removing the Provisioning user.

Procedure

1. Go to [Admin Center](#) > [Manage Provisioning Access](#).
2. Select one or more users.
3. Click the "delete" icon.
4. Confirm that you want to remove the specified Provisioning users by clicking [OK](#).

Results

The specified Provisioning users can no longer access Provisioning for your instance. The specified Provisioning users are not notified.

Task overview: [Provisioning Access Management \[page 4\]](#)

Related Information

[Provisioning \[page 4\]](#)

[Viewing Users with Provisioning Access \[page 7\]](#)

[Approving a New Provisioning User \[page 8\]](#)

[Super Admin Management \[page 12\]](#)

3 Super Admin Management

You can use the [Manage Provisioning Access](#) tool to view super admins in your system and the Provisioning user who created them.

[Super Administrators \[page 12\]](#)

A super administrator, or "super admin", is an admin user that is created in the Provisioning application for your system and who has special access and administrative privileges.

[Viewing Super Admins with Access to Your System \[page 13\]](#)

View super admins and the Provisioning user who created them, using the [Manage Provisioning Access](#) tool.

[Removing a Super Admin User \[page 14\]](#)

Remove a super admin user that was created in Provisioning, according to your regular deactivation process.

[Creating a Super Admin User in Provisioning \[page 16\]](#)

Create a super admin user in the Provisioning application, for a specific customer instance, so that you can access the system and grant necessary permissions to other users.

3.1 Super Administrators

A super administrator, or "super admin", is an admin user that is created in the Provisioning application for your system and who has special access and administrative privileges.

Super admins are typically created by SAP consultants or partners during the implementation phase or during migration to role-based permissions. A super admin user automatically has the ability to:

- Access your system
- Manage system permissions
- Grant or deny other users the ability to manage system permissions

Super admins are only necessary **before** system permissions have been set up properly. After permissions have been set up and the relevant system administrators have been given the ability to manage these permissions, the super admin user account can be deactivated.

Apart from the fact that they are created in Provisioning and have certain privileges granted by default, a super admin user is like any other user in your system and can be managed according to your regular process. For example:

- They may have other permissions that you have granted to "everyone" or to a target population they belong to.
- They can only access your system by methods you allow (manual login, secondary login, SSO).
- You can reset their password.
- They can be deactivated or purged.

Parent topic: [Super Admin Management \[page 12\]](#)

Related Information

[Viewing Super Admins with Access to Your System \[page 13\]](#)

[Removing a Super Admin User \[page 14\]](#)

[Creating a Super Admin User in Provisioning \[page 16\]](#)

3.2 Viewing Super Admins with Access to Your System

View super admins and the Provisioning user who created them, using the [Manage Provisioning Access](#) tool.

Prerequisites

You have [View Provisioning Access](#) permission.

Procedure

1. Go to [Admin Center](#) > [Manage Provisioning Access](#).
2. Refer to the [Super Admins Created](#) column to see how many super admin users have been created in Provisioning by each Provisioning user.
3. For each row where 1 or more super admin users are indicated, click the number to see more information about each one.

For each super admin user, you can see:

- ID
- Username
- Email
- Status

Next Steps

Now that you know all of the super admin users that exist in your system, you can take action as needed. You can remove unnecessary super admin users according to your standard deactivation process.

Task overview: [Super Admin Management \[page 12\]](#)

Related Information

[Super Administrators \[page 12\]](#)

[Removing a Super Admin User \[page 14\]](#)

[Creating a Super Admin User in Provisioning \[page 16\]](#)

3.3 Removing a Super Admin User

Remove a super admin user that was created in Provisioning, according to your regular deactivation process.

Context

A super admin user account differs from other user accounts only in the way it is created and in the special privileges it has by default. Once created, it can be managed in the same way as any other user account, according to your regular process.

Procedure

1. Set the super admin user's employment status to **inactive** to deactivate the user and prevent access to your system.
2. Use the data purge function to permanently remove the inactive user from your system.

Task overview: [Super Admin Management \[page 12\]](#)

Related Information

[Super Administrators \[page 12\]](#)

[Viewing Super Admins with Access to Your System \[page 13\]](#)

[Creating a Super Admin User in Provisioning \[page 16\]](#)

3.3.1 Setting User Status to Inactive

Users in SAP SuccessFactors can have either an active or inactive status. By default, the status of all of users is set to active when they are initially added to SAP SuccessFactors. If you want to freeze a user account, you can set the user as inactive in the system.

Prerequisites

Before you use the UI-based method to deactivate a user who is a manager, you need to do a manager transfer, which forwards in-progress forms to a new manager. To set up a manager transfer, use the Automatic Manager Transfer tool in Performance Management.

Context

Setting a user as inactive means that no changes can be made to the account. You can change user status one by one using the UI, or modify multiple user statuses in a file and upload it to SAP SuccessFactors.

Procedure

- Use the UI-based method.
 - a. Go to [Admin Center](#).
 - b. In the tools search field, type [Manager Users](#).
 - c. Search the user that you want to deactivate.
 - d. Click the user's name. In the [Edit User](#) window, select [No](#) for the [Active](#) field.
 - e. Click [Save](#) to save your change.
- Use the file-based method.
 - a. Prepare your user data file and change the [Status](#) field to inactive in the file.
 - b. Import the user data file as you would for any other data change.

Note

If any of the deactivated users are managers, you can configure automatic manager transfer using the import options.

3.4 Creating a Super Admin User in Provisioning

Create a super admin user in the Provisioning application, for a specific customer instance, so that you can access the system and grant necessary permissions to other users.

Prerequisites

You have Provisioning access to the instance.

→ Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Product Support.

Procedure

1. Log into Provisioning and select the company instance you wish to access.
2. Go to ► [Edit Company Settings](#) ► [Company Settings](#) ►.
3. Search or scroll down the page to find the section with "super admin" settings.
4. Provide **all** of the following information.

Setting	Description
Admin Username	Determines both Username and User ID of the super admin user.
Admin Password	Password with which super admin can access your system.
Admin First Name	First name of super admin as it appears in the system.
Admin Last Name	Last name of super admin as it appears in the system.
Admin Email	Email address to which super admin receives notifications.
Use PWD to log in to SAP SuccessFactors	Once it is checked, the newly created super admin can log into the system using username and password.

ⓘ Note

This **ONLY** applies to the instance that has enabled Partial Organization SSO.

Setting	Description
Confirmation of customer approval	<p>Provisioning user must check a box confirming that they have received approval from the affected customer for the creation of a super admin user account.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px;"> <p>Note</p> <p>As a Provisioning user, it is your responsibility to obtain this approval before creating a super admin. You cannot proceed without confirming that you have done so.</p> </div>
Customer Email Address	<p>Customer email address that receives notification when the super admin account is created.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px;"> <p>Note</p> <p>This should be the email address of one person who provided the customer approval. You can only send notification to one address.</p> <p>As a Provisioning user, it is your responsibility to notify the customer and share this information with more people if necessary.</p> </div>

5. Select *Create Admin*.

Note

You can only proceed to create a super admin if you have provided all of the required information. If not, this action is disabled.

6. Save your changes.

Results

The super admin user account is created and the customer is notified at the email address provided.

Task overview: [Super Admin Management \[page 12\]](#)

Related Information

[Super Administrators \[page 12\]](#)

[Viewing Super Admins with Access to Your System \[page 13\]](#)

[Removing a Super Admin User \[page 14\]](#)

4 IP Restriction Management

As an administrator, you can add or remove IP restrictions, using the [IP Restriction Management](#) tool in Admin Center.

You can use this tool to specify the IP addresses from which users are allowed to access your instance. You can add any number of single IP addresses or a range of sequential IP addresses to the allowlist.

This is a universal feature, available in all SAP SuccessFactors instances. However, to access this tool, you must first be granted [IP Restriction Management](#) permission.

[IP Restrictions \[page 18\]](#)

IP restrictions are a specified list of IP addresses from which users can access your system.

[Adding an IP Restriction \[page 19\]](#)

Add one or more IP addresses to the list addresses from which users are allowed to access your instance.

[Excluding External Users from IP Restrictions \[page 20\]](#)

Exclude external users from IP restrictions so that they can access your instance from any IP address.

4.1 IP Restrictions

IP restrictions are a specified list of IP addresses from which users can access your system.

As an administrator, you can manage the IP restrictions list. Anyone who attempts to access your system from an unspecified IP address is presented with an error message and redirected to the login page.

IP restrictions take effect as soon as one or more IP addresses is added to the restrictions list. If no IP restrictions are added, users can access your system from any IP address.

Parent topic: [IP Restriction Management \[page 18\]](#)

Related Information

[Adding an IP Restriction \[page 19\]](#)

[Excluding External Users from IP Restrictions \[page 20\]](#)

4.2 Adding an IP Restriction

Add one or more IP addresses to the list addresses from which users are allowed to access your instance.

Prerequisites

You have *IP Restriction Management* permission.

Procedure

1. Go to [Admin Center](#) > [IP Restriction Management](#).
2. Click the plus icon to open the *Add IP Address* dialog.
3. Select one of the following options:

Option	Description
<i>Single IP Address</i>	Select this option to enter a single IP address. For example: 2.2.2.34
<i>IP Address Range</i>	Select this option to define a range of IP addresses. For example: 0.0.0.0 to 255.255.255.254

Note

Please enter IPv4 addresses only. IPv6 is not supported.

4. Enter the IP address or address you want to allow.
5. Click *Save*.

Task overview: [IP Restriction Management \[page 18\]](#)

Related Information

[IP Restrictions \[page 18\]](#)

[Excluding External Users from IP Restrictions \[page 20\]](#)

4.3 Excluding External Users from IP Restrictions

Exclude external users from IP restrictions so that they can access your instance from any IP address.

Prerequisites

You have *IP Restriction Management* permission.

Procedure

1. Go to [Admin Center](#) > [IP Restriction Management](#).
2. Click the gear icon to open the *IP Restriction Settings* dialog.
3. Select one of the following options:

Option	Description
Turn off the IP restriction for external 360 Reviews users	If you are using 360 Reviews with Performance & Goals, this option excludes external raters from your configured IP restrictions.
Turn off the IP restriction for external onboarding users	If you are using SAP SuccessFactors Onboarding, this option excludes Pre-Day 1 external onboarding users from your configured IP restrictions.
Turn off the IP restriction for external learning users	If you are using SAP SuccessFactors Learning Extended Enterprise, this option excludes external learning users from your configured IP restrictions.

4. Save your changes.

Task overview: [IP Restriction Management \[page 18\]](#)

Related Information

[IP Restrictions \[page 18\]](#)

[Adding an IP Restriction \[page 19\]](#)

5 Support Access Management

As an administrator, you can use the [Manage Support Access](#) admin tool to grant or remove support access to a specified user account. You can check the role-based permissions (RBP) administrator access of support accounts, and further restrict the RBP administrator access of support accounts.

When you grant support access to an account, you must set a date when support access expires. The validity period can't exceed 2 years.

The [Manage Support Access](#) admin tool is available in all SAP SuccessFactors instances that have secondary login enabled. However, to access this tool, you must be granted [Manage Support Access](#) permission.

[Support Access with Secondary Login \[page 21\]](#)

Support access is the ability of an SAP SuccessFactors employee or partner to access your instance by logging into a specified user account using secondary login. Secondary login is a feature in the Provisioning application that enables people with support access to log into your instance with the specified user account directly from Provisioning, without using the regular login page.

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

Enable the secondary login feature so that Provisioning users can access the specified instance and administrators can manage support access to that instance.

[Granting Support Access to a Specified User Account \[page 23\]](#)

Grant support access to a specified user account so that secondary login users can access it.

[Removing Support Access to User Accounts \[page 24\]](#)

Remove support access to a specified user account from secondary login users.

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

You can check the RBP administrator access of support accounts, and further restrict the RBP administrator access of support accounts.

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

As an SAP employee or partner who has been granted support access, log into a customer instance as a specified user.

5.1 Support Access with Secondary Login

Support access is the ability of an SAP SuccessFactors employee or partner to access your instance by logging into a specified user account using secondary login. Secondary login is a feature in the Provisioning application that enables people with support access to log into your instance with the specified user account directly from Provisioning, without using the regular login page.

As a customer administrator, you can control who can access which user accounts in your instance with secondary login. You can grant temporary access to SAP SuccessFactors employees or partners, during implementation or during the investigation of an issue. Typically, support access is granted to a shared user account that can be accessed by multiple people. We recommend that you provide granular access to user accounts on a need-to-know basis for each particular troubleshooting or administrative task.

Note

As an SAP employee or partner with both Provisioning access and support access, you can use secondary login to access to a customer's instance.

When Single Sign-On is enabled, secondary login is the recommended method for SAP employees and partners to access a customer instance. It is **not** necessary to enable Partial Organization SSO or request login access through the customer's SSO portal.

Parent topic: [Support Access Management \[page 21\]](#)

Related Information

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

[Granting Support Access to a Specified User Account \[page 23\]](#)

[Removing Support Access to User Accounts \[page 24\]](#)

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

5.2 Enabling Secondary Login and Support Access Management

Enable the secondary login feature so that Provisioning users can access the specified instance and administrators can manage support access to that instance.

Procedure

1. Go to ► [Admin Center](#) ► [Platform Feature Settings](#) ► and check the box for *Enable Secondary Login Feature* and save your changes.

Note

By default, *Enable Secondary Login Feature* is not enabled.

2. Grant the *Manage Support Access* permission to the appropriate people or roles using the *Manage Permission Roles*.
3. Save.

Results

Secondary login is now enabled for the instance. People with permission can now use the [Manage Support Access](#) tool.

Task overview: [Support Access Management \[page 21\]](#)

Related Information

[Support Access with Secondary Login \[page 21\]](#)

[Granting Support Access to a Specified User Account \[page 23\]](#)

[Removing Support Access to User Accounts \[page 24\]](#)

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

5.2.1 Permission to Manage Support Access

If secondary login is enabled in your instance, it is a good idea to give some administrators in your company the [Manage Support Access](#) permission.

This permission enables you to use the [Manage Support Access](#) tool to grant or remove support access, via secondary login, to a specified user account.

5.3 Granting Support Access to a Specified User Account

Grant support access to a specified user account so that secondary login users can access it.

Prerequisites

You've [Manage Support Access](#) permission.

Procedure

1. Go to [Admin Center](#) > [Manage Support Access](#) and use the available search filters to find the user or users for whom you want to grant login access.

You can see two tabs, *Valid List* and *Expired List* on the *Manage Support Access* page.

2. Choose *Add*.

A *Grant Access* popup displays.

3. Search for a user.
4. Choose whether to allow the support account to edit RBP configurations or not.

If the user account doesn't have *Role-Based Permissions Admin Access (Edit)* permission in *Manage Role-Based Permission Access*, even if you choose *Yes* in this field, it doesn't take effect upon saving. However, if the user is granted the *Role-Based Permissions Admin Access (Edit)* later, the support account can edit RBP settings immediately.

5. Choose an expiration date.

You can choose a date that is within 2 years.

Results

Your Product Support contact, or other SAP consultant or partner, has login access to the specified user accounts until the expiration date you set.

Task overview: [Support Access Management \[page 21\]](#)

Related Information

[Support Access with Secondary Login \[page 21\]](#)

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

[Removing Support Access to User Accounts \[page 24\]](#)

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

5.4 Removing Support Access to User Accounts

Remove support access to a specified user account from secondary login users.

Prerequisites

You've *Manage Support Access* permission.

Procedure

1. Go to ► [Admin Center](#) ► [Manage Support Access](#) and use the available search filters to find the user or users for whom you want to grant login access.

You can see two tabs, *Valid List* and *Expired List* on the *Manage Support Access* page.

2. Select users in the *Valid List* tab.
3. Choose *Remove*.

A double-confirmation popup displays.

4. Choose *Yes*.

Task overview: [Support Access Management \[page 21\]](#)

Related Information

[Support Access with Secondary Login \[page 21\]](#)

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

[Granting Support Access to a Specified User Account \[page 23\]](#)

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

5.5 Checking Role-Based Permissions Administrator Access of a Support Account

You can check the RBP administrator access of support accounts, and further restrict the RBP administrator access of support accounts.

Prerequisites

You've *Manage Support Access* permission.

Procedure

1. Go to ► [Admin Center](#) ► [Manage Support Access](#) and use the available search filters to find the user or users for whom you want to grant login access.

You can see two tabs, *Valid List* and *Expired List* on the *Manage Support Access* page.

2. Choose *Check Access* in the *Actions* column.

A *Check Access* popup displays.

- A message strip displays on the top, informing you whether the user account has RBP edit access or not in [Admin Center > Manage Role-Based Permission Access](#).
- *Manage Role-Based Permission Access*: whether the user account has RBP edit access, view access, or no access in *Manage Role-Based Permission Access*.
- *“Allow to Edit RBP” in Manage Support Access*: whether the user account is allowed to edit RBP settings in *Manage Support Access*. Available values are *Yes* and *No*.

Note

This selection is specific to users logging in SAP SuccessFactors using secondary login only. Also, whether a support account has RBP administrator edit access or view access depends on a combination of configurations in the *Manage Role-Based Permission Access* and the *Manage Support Access* admin tools. Here are the details:

Manage Role-Based Permission Access	“Allow to Edit RBP” in Manage Support Access	Results
Role-Based Permission Admin (Edit)	Yes	The user account can edit RBP settings.
Role-Based Permission Admin (Edit)	No	The user account can only view RBP settings.
Role-Based Permission Admin (View)	Yes	The user account can only view RBP settings.
Role-Based Permission Admin (View)	No	The user account can only view RBP settings.
The user account isn't listed in the <i>Manage Role-Based Permission Access</i> page.	Yes	The user account doesn't have RBP administrator access.
The user account isn't listed in the <i>Manage Role-Based Permission Access</i> page.	No	The user account doesn't have RBP administrator access.

3. Choose *Close*.

Task overview: [Support Access Management \[page 21\]](#)

Related Information

[Support Access with Secondary Login \[page 21\]](#)

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

[Granting Support Access to a Specified User Account \[page 23\]](#)

[Removing Support Access to User Accounts \[page 24\]](#)

[Logging In to a Support Access-Enabled Account with Secondary Login \[page 27\]](#)

5.6 Logging In to a Support Access-Enabled Account with Secondary Login

As an SAP employee or partner who has been granted support access, log into a customer instance as a specified user.

Prerequisites

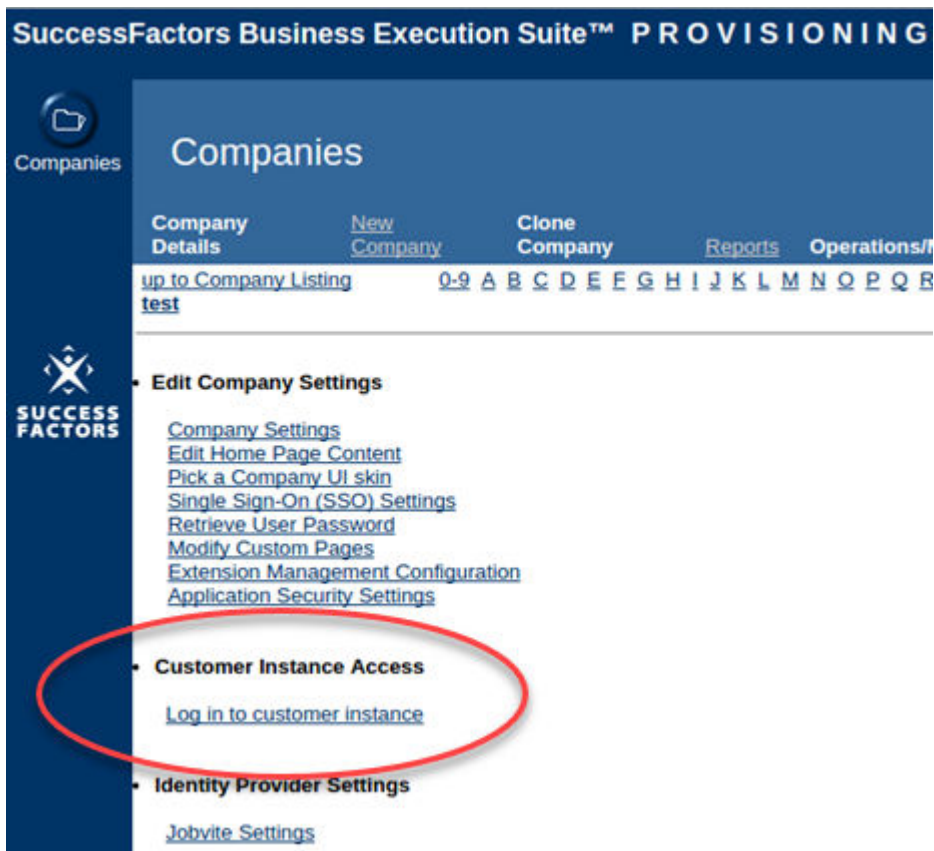
- [Enable Secondary Login Feature](#) is enabled.
- You have access to Provisioning.

→ Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Product Support.

Procedure

1. Log into Provisioning and select the company instance you wish to access.
2. Click [Log in to customer instance](#), under [Customer Instance Access](#).



3. Enter your username on the [Secondary Login](#) page.
4. Click [Login](#).
5. Select [OK](#) to confirm the information is correct, or cancel if it is not.

Results

A new window pops up and you are logged in as the specified user.

Task overview: [Support Access Management \[page 21\]](#)

Related Information

[Support Access with Secondary Login \[page 21\]](#)

[Enabling Secondary Login and Support Access Management \[page 22\]](#)

[Granting Support Access to a Specified User Account \[page 23\]](#)

[Removing Support Access to User Accounts \[page 24\]](#)

[Checking Role-Based Permissions Administrator Access of a Support Account \[page 25\]](#)

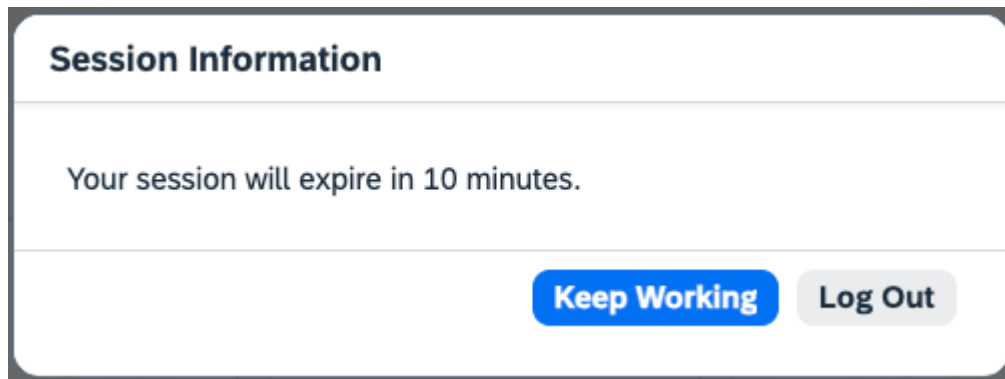
6 Session Timeout

Understand the concept of session timeout to better work with your SAP SuccessFactors instances.

When a user logs in to an SAP SuccessFactors instance, a browser session is created for the user so that they can browse and interact with the system. When the user doesn't perform any action (remains inactive) for a prolonged period of time, the system automatically ends the session. The user must log in again to continue working. Session timeout refers to the system event that ends a browser session after it expires.

In SAP SuccessFactors, the default time before a session gets timed out is 30 minutes. Users get a warning 10 minutes before session timeout happens. They have the option to either keep working, which resets the timer back to 30 minutes, or log out immediately.

Here's an example of the warning popup before session timeout happens:



ⓘ Note

The default timeout values are valid for desktop applications only. API and mobile applications follow different session timeout mechanisms. For more information, see the Related Information section.

Default timeout values can only be changed in Provisioning. If you want to change the default values, contact your implementation partner or Product Support.

Related Information

[Timeouts](#)

Change History

Learn about changes to the documentation for Managing Instance Access in recent releases.

2H 2023

Type of Change	Description	More Info
Changed	We've moved the Change History to the end of the guide.	Instance Access Management [page 3]
Added	We added a new overview topic for the guide.	Instance Access Management [page 3]
Added	We added information on the redesigned Manage Support Access tool.	Support Access Management [page 21] Granting Support Access to a Specified User Account [page 23] Removing Support Access to User Accounts [page 24] Checking Role-Based Permissions Administrator Access of a Support Account [page 25]
Added	We added a new topic to explain how session timeout works.	Session Timeout [page 29]

1H 2023



Type of Change	Description	More Info
Added	Added a link to the Managing User Information guide for details about how to add a new user.	Approving a New Provisioning User [page 8]
Added	Added information about the <i>Show Users with Valid Support Access</i> filter option.	Granting Support Access to a Specified User Account [page 23] Removing Support Access to User Accounts [page 24]
Changed	Updated the label name of <i>Turn off the IP restriction for 360 Multi-Rater external users</i> into <i>Turn off the IP restriction for external 360 Reviews users</i>	Excluding External Users from IP Restrictions [page 20]

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.